



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,983	03/15/2004	G. Glenn Henry	CNTR.2073	1410
23660 7590 07/26/2010 HUFFMAN LAW GROUP, P.C. 1900 MESA AVE. COLORADO SPRINGS, CO 80906				
EXAMINER TRAORE, FATOUMATA				
ART UNIT 2436		PAPER NUMBER		
NOTIFICATION DATE 07/26/2010		DELIVERY MODE ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOHLG@me.com

Office Action Summary

Application No.

10/800,983

Applicant(s)

HENRY ET AL.

Examiner

FATOUMATA TRAORE

Art Unit

2436

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 April 2010.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,4-6,8-15,17-20 and 22-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,4-6,8-15,17-20 and 22-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB06)
Paper No(s)/Mail Date 05/20/2010
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(c), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(c) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 04/22/2010 has been entered.

Status of Claims

2. Claims 1, 17 and 22 have been amended. Claims 2, 3, 7, 16, 21 and 26 have been cancelled. Claims 1, 4-6, 8-15, 17-20 and 22-25 are pending and have been considered below.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 4-6, 8-15, 17-20 and 22-25 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1, 4-6, 8, 13, 17-20 and 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Verbauwhede (US 2003/0202658) in view of Wichman et al (US 5,884,062).

Claims 1, 17 and 22: Verbauwhede disclose an apparatus and a method for performing cryptographic operations, comprising:

An X86-compatible microprocessor, comprising:

- i. An instruction register within a x86-compatible microprocessor having a single atomic cryptographic instruction disposed therein, wherein said single, atomic cryptographic instruction is arranged according to the instruction format for execution on said x86-compatible microprocessor, (*column 3, lines 40-45*) and wherein said single, atomic cryptographic instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program, and wherein said single, atomic cryptographic instruction prescribes an encryption operation, and wherein said cryptographic instruction prescribes that a user-generated key schedule be employed for execution of said encryption operation, and wherein said encryption operation that is prescribed by said single, atomic cryptographic instruction comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks (*AES architecture to implement Electronic Code Book, Cipher Block Chaining, Output Feedback and Cipher Feedback mode*) (*paragraphs [0019], [0034] and [0036]*);
- ii. A keygen unit, operatively coupled to said instruction register, configured to direct said x86-compatible microprocessor to load said user-generated key schedule (*paragraph [0022]*); and

iii. An execution unit, operatively coupled to said keygen unit, configured to employ said user-generated key schedule to execute said encryption operation (*paragraphs [0021], [0031], [0032]*), said execution unit comprising:

A cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit (*paragraph [0036]*).

Verbauwhede do not explicitly specify wherein said cryptographic wherein said x86-compatible microprocessor executes said application program. However Wichman et al disclose an apparatus and method, which further disclose wherein said single, atomic cryptographic instruction is part of an application program, and wherein said x86-compatible microprocessor executes said application program(column 7, lines 45-60 column 8, lines 51-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Verbauwhede such as to use the x86-compatible microprocessor to execute a single atomic instruction. The motivation of doing so would have been to improve performance of the microprocessor as taught by Wichman et al (column 1, lines 10-20).

Claims 4, 18 and 24: Verbauwhede and Wichman et al disclose an apparatus and a method for performing cryptographic operation as in claims 1, 17 and 22 above, and Verbauwhede further discloses, wherein said user-generated key schedule is stored in memory (*paragraph [0022]*).

Claims 5, 19 and 25: Verbauwhede and Wichman et al disclose an apparatus and method for performing cryptographic operation as in claims 1, 17 and 22 above, and Verbauwhede further disclose, wherein said user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm (*paragraphs [0030], [0032]*).

Claims 6, 20 and 23: Verbauwhede and Wichman et al disclose an apparatus and a method as in claims 1, 17 and 22 above, and Verbauwhede further disclose that said keygen unit is configured to interpret a key generation field within a control word, which is referenced by said cryptographic instruction (*paragraph [0034]*).

Claim 8: Verbauwhede and Wichman et al disclose an apparatus as in claim 1 above and Verbauwhede further disclose that said cryptographic instruction implicitly references a plurality of registers within said x86-compatible microprocessor (*execution unit*) (*paragraphs [0021], [0024]*).

Claim 13: Verbauwhede and Wichman et al disclose an apparatus and a method as in claim 8 above, and Verbauwhede further disclose that said user-generated cryptographic key schedule comprises said cryptographic key data (*paragraphs [0020]-[0024]*).

6. Claims 9-12, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Verbauwhede (US 2003/0202658) in view of Wichman et al (US 5,884,062) in further view of Kessler et al (US 6,789,147).

Claims 9-11: Verbauwhede and Wichman et al disclose an apparatus as in claim 8 above, while neither of them explicitly discloses that said cryptographic instruction..... a

plurality of input text blocks, However, Kessler et al disclose that said cryptographic instruction implicitly references a plurality of registers, which include a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of a plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished ; and a second register wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks said third register indicate a number of text blocks within a plurality of input text blocks *(each execution unit includes a register file block that includes data to be operated on by the corresponding cryptographic algorithm) (column 9, lines 18-40; Fig. 8).*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Verbauwhede and Wichman et al such as to include a plurality of register. The motivation of doing so would have been to preserve data privacy and protect sensitive data during its transmission during across different communication networks as taught by Kessler et al (column 1, lines 15-25).

Claim 12: Verbauwhede and Wichman et al disclose an apparatus as in claim 8 above, while neither of them explicitly discloses that said plurality of registers comprises said one of the cryptographic operations. However, Kessler et al disclose that said plurality of registers comprises a fourth register, wherein contents of said fourth register

comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations (*column 9, lines 18-40; Fig. 5 and Fig. 8*).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Verbauwhede and Wichman et al such as to include a plurality of register. The motivation of doing so would have been to preserve data privacy and protect sensitive data during its transmission during across different communication networks as taught by Kessler et al (*column 1, lines 15-25*).

Claim 14: Kessler et al and Christie et al disclose an apparatus as in claim 8 above, while neither of them explicitly discloses that said plurality of registers comprises a said cryptographic operations, However, Kessler et al disclose that said plurality of registers comprises a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations(*cryptographic operation such as RC4*) (*column 9, lines 18-40; Fig. 5 and Fig. 8*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Verbauwhede and Wichman et al such as to include a plurality of register. The motivation of doing so would have been to preserve data privacy and protect sensitive data during its transmission during across different communication networks as taught by Kessler et al (*column 1, lines 15-25*).

Claim 15: Verbauwhede and Wichman et al disclose an apparatus as in claim 8 above, while neither of them explicitly discloses that said plurality of registers comprises execution of said one of the cryptographic operations, However, Kessler et al disclose that said plurality of registers comprises a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises: a key size field ($nk = \text{key size}$), configured to specify said one of a plurality of cryptographic key sizes to be employed during execution of said one of the cryptographic operations (*cryptographic operation such as RC4*) (column 9, lines 18-40; Fig. 5 and Fig. 8). The examiner notes that it is inherent for the control word to be stored in memory because the key expansion block uses it for generating a round key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teaching of Verbauwhede and Wichman et al such as to include a plurality of register. The motivation of doing so would have been to preserve data privacy and protect sensitive data during its transmission during across different communication networks as taught by Kessler et al (column 1, lines 15-25).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685.

The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Thursday, July 15, 2010.

/F. T./

Examiner, Art Unit 2436

/David García Cervetti/

Primary Examiner, Art Unit 2436